ABSTRACT

The present invention pertains to a transmission apparatus (110) for generating an encrypted text by encrypting a plaintext, which includes a parameter storage unit (112) for storing a random parameter (the number of terms whose coefficients indicate 1) adapted to an encryption key and an encryption apparatus and a decryption apparatus; encryption unit (116) for generating, from the plaintext, the encrypted text using the encryption key and the random parameter stored in the parameter storage unit (112), complying with an encryption algorithm based on the NTRU method; and a key updating unit (118) for updating the random parameter stored in the parameter storage unit (112) and the encryption key, as time passes.